1. Objetivo

Estabelecer diretrizes para segurança de todos os ativos da empresa, visando assegurar que todas as informações processadas, transferidas e/ou armazenadas recebam a proteção e o tratamento adequado.

2. Escopo

Esta Política é aplicável a todos os colaboradores, fornecedores e prestadores de serviço, abrangendo todos os dados, inclusive os do ambiente PCI-DSS (*Payment Card Industry - Data Security Standard*) .

3. Estrutura

A área de Segurança da Informação, sob gestão do Diretor Presidente, é responsável por zelar pela aplicação das diretrizes desta política.

4. Atribuições

A Diretoria deve zelar pela aprovação do acesso, compartilhamento, divulgação e manutenção do sigilo das informações, sendo vedada a divulgação de quaisquer tipos de informações para terceiros, sem a prévia autorização. A execução dessas atividades está sob execução da área de Segurança da Informação.

A área de Segurança da Informação é responsável pela criação de controles e processos, visando a melhoria contínua da proteção das informações, disseminar a cultura de segurança da informação e por garantir o efetivo cumprimento desta política, ressaltando o uso ético, seguro e legal das informações.

Deve também orientar e informar os colaboradores, fornecedores e prestadores de serviços, para que sejam aptos a comunicá-los sempre que identificarem possíveis violações dos controles definidos nesta política e nos procedimentos complementares a este respeito, cumprindo a legislação e demais instrumentos regulamentares relacionados às suas atividades profissionais, zelando pela guarda e proteção das informações, não as divulgando sem a devida aprovação e utilizando os ativos, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas.

A área de *Compliance* é responsável pela divulgação desta Política e deve ser envolvida sempre que houver qualquer descumprimento das definições expostas nesta Política, para dar seguimento a aplicação das devidas tratativas.

A área de P&C deve cumprir os controles de segurança da informação relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores.

A área de Assuntos Legais é responsável por validar os controles de segurança da informação aplicáveis aos contratos, tais controles estão estabelecidos no Anexo de Segurança da Informação. Quando aplicável, devem orientar a área de Segurança da Informação neste quesito.

5. Diretrizes de Segurança para Colaboradores e Prestadores de serviços

5.1. Uso do e-mail e *Internet*

O e-mail corporativo (@picpay.com) deve ser utilizado somente para fins profissionais e em alinhamento aos interesses da empresa, observado o Código de Ética e Conduta - CODEC.

Todos os colaboradores têm acesso a *internet* para desempenho das atividades corporativas e o uso moderado da navegação na *internet* é de responsabilidade do próprio colaborador.

O PicPay reserva o direito de monitorar e auditar, sem aviso prévio, as informações acessadas e manipuladas, podendo utilizar tais evidências para detectar e analisar incidentes ou prova judicial, se necessário.

Essa medida visa preservar os direitos da empresa e prover um ambiente seguro e controlado aos colaboradores, fornecedores e prestadores de serviço.

5.2. Uso de Rede Sociais

Não é permitido ao colaborador comentar ou responder em nome da empresa, divulgar ou compartilhar informações, fotos, vídeos e gravações no ambiente de trabalho ou em eventos corporativos, que exibam documentos e informações internas, exceto quando expressamente autorizado.

6. Disposições Gerais

6.1. Controle de acesso

Os acessos físicos devem ser protegidos por controles apropriados de entrada e saída, com o objetivo de assegurar que somente pessoas autorizadas tenham acesso às dependências da empresa.

Os acessos lógicos, devem ter controles de criação, avaliação e revogação, bem como permitir, a cada colaborador, apenas os acessos necessários à executar suas atividades. O login e senha fornecidos são de uso pessoal, intransferível, limitados às finalidade designada e devidamente autorizados, de acordo com suas funções e responsabilidades.

6.2. Rastreabilidade da informação

Toda informação da instituição classificada como confidencial ou restrita deve possuir *logs* para monitorar o acesso, a inclusão e a alteração dessas informações.

As aplicações que processam dados sensíveis, devem gerar e armazenar *logs* para fins de auditoria.

6.3. Classificação e tratamento da informação

As informações criadas internamente ou recebidas de fontes externas, independentemente do formato, como documentos em papel, armazenados eletronicamente ou transmitidas verbalmente, devem ser classificadas conforme sua criticidade, o custo financeiro e de risco de imagem da exposição dessas informações.

Será utilizada a metodologia, para a efetivação da classificação, conforme previsto nos normativos internos.

6.4. Respostas a Incidentes de Segurança da Informação

Incidente de Segurança da Informação é toda ocorrência, confirmada ou sob suspeita, que pode comprometer a confidencialidade, integridade e disponibilidade no ambiente.

Todo incidente de segurança da informação deve ser reportado para análise da área de Segurança da Informação e devem ser classificados conforme sua criticidade para continuidade do negócio, o impacto na usabilidade do serviço de pagamento e o impacto financeiro.

Os incidentes classificados como relevantes devem ser registrados em local específico, ser analisados quanto à causa e o impacto, assim como o controle dos seus efeitos para as atividades de pagamento.

6.5. Proteção contra agentes maliciosos

Todo computador da instituição deve possuir instalada a solução de *antivírus* corporativo e a área de Segurança da Informação tem autonomia para, caso julguem necessário, tomar medidas pró-ativas para combater ou prevenir a disseminação de agentes maliciosos.

6.6. Controles criptográficos

A criptografia utilizada é objeto de análise e aprovação da área de Segurança da Informação, que zela pela eficiência comprovada deste controle.

6.7. Gestão de continuidade de negócios

O PicPay possui um conjunto de planos de continuidade de negócios permitindo, assim, a redução da exposição aos riscos de perdas financeiras e impactos negativos de imagem no mercado.

Visando a manutenção de um processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas, existem controles de *backup,* garantindo a continuidade do negócio em caso de falhas ou incidentes.

Para mitigação dos riscos de continuidade das operações e os riscos inerentes à segurança da informação de forma a proteger a confidencialidade, a integridade e a disponibilidade das informações armazenadas, transmitidas e/ou manipuladas, deverão ser elaborados os cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados, levando em consideração a periodicidade dos testes, a criticidade dos sistemas utilizados, o impacto desses sistemas na prestação dos serviços de pagamentos, a sensibilidade das informações armazenadas, transmitidas ou processadas.

6.8. Fornecedores e Prestadores de Serviço

Todos os fornecedores e prestadores de serviço devem ser avaliados levando em consideração as estratégias de segurança e privacidade, relevância e classificação de riscos.

6.9. *Cloud Computing*

A área de Segurança da Informação deve zelar pela segurança dos processos, serviços e sistemas em ambiente de *Cloud Computing*, abrangendo todas as informações processadas, transferidas ou armazenadas.

6.10. Desenvolvimento Seguro

As áreas de Segurança da Informação e Engenharia devem zelar para que as aplicações sejam desenvolvidas de forma segura considerando todas as etapas do ciclo de desenvolvimento de software, compreendendo controles a serem implementados, monitorados, revisados e aprimorados.

6.11. Disseminação da Cultura de Segurança Cibernética

A área de Segurança da Informação é responsável pela implementação de um programa de treinamentos e conscientização de segurança da informação para todos os colaboradores, fornecedores e prestadores de serviço.

Além disso, deve apoiar um programa de prestação de informação na utilização de produtos e serviços.